

IN THE CLAIMS:

1. (Currently Amended) A particular plaintext detector for detecting whether plaintext to be inputted into a predetermined encryption algorithm satisfies a predetermined condition, the particular plaintext detector comprising:

a receiving part for receiving ~~the plaintext~~ a plurality of plaintexts sequentially;

5 a counter part for separating a predetermined part from a bit string forming the ~~plaintext~~ each of the plurality of plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted ~~plaintext~~ having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts plaintexts each of which has the same value of the fixed part, and

10 storing ~~[[it]]~~ the number as a separate count; and

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number.

2. (Currently Amended) A particular plaintext detector for detecting whether ~~plaintext~~ each of a plurality of plaintexts, to be inputted into a block encryption algorithm, satisfies a predetermined condition, the block encryption algorithm receiving and stirring ~~plaintext~~ each of the plurality of plaintexts with a key step by step to perform encryption and

5 outputting ciphertext, the particular plaintext detector comprising:

a receiving part for receiving a plurality of the plaintext plaintexts sequentially;

a counter part for separating a predetermined part from a bit string forming the ~~plaintext~~ each of the plurality of plaintexts into a fixed part and a remaining part into a variable

part, counting the number of inputted plaintext having a value of the fixed part included in a set  
10 of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality  
of the values of the fixed parts plaintexts each of which has the same value of the fixed parts, and  
storing it as a separate count; and

a detecting part for outputting a detection signal that shows the encryption  
algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a  
15 predetermined number.

3. (Currently Amended) A particular plaintext detector for detecting whether  
plaintext each of a plurality of plaintexts to be inputted into a KASUMI type encryption  
algorithm having a stirring step satisfies a predetermined condition, the KASUMI type  
encryption algorithm equal to KASUMI which is a block encryption algorithm that receives the  
5 plurality of plaintext plaintexts sequentially, has a plurality of stirring steps for [[stir]] stirring  
with a key, and performs encryption step by step to output ciphertext, the particular plaintext  
detector comprising:

a receiving part for receiving the plurality of the plaintext plaintexts sequentially;

a counter part for separating 17th to 32nd bits of the plaintext each of the plurality  
10 of plaintexts from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof  
into a variable part, counting the number of inputted plaintext having a value of the fixed part  
included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed  
parts at every set of the values of the fixed parts plaintexts each of which has the same value of  
the fixed part, and storing it as a separate count; and

15           a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a predetermined number.

4.       (Currently Amended) A filter apparatus for limiting an output of ciphertext from an encryption algorithm that receives ~~plaintext~~ a plurality of plaintexts ~~to output~~ and outputs ciphertext, the filter apparatus comprising:

          a receiving part for receiving the plurality of the plaintext ~~plaintexts~~ sequentially;

5           a counter part for separating a predetermined part from a bit string forming ~~the plaintext~~ each of the plurality of plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted ~~plaintext~~ having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts ~~plaintexts~~ each of which has the same value of the fixed part, and  
10       storing it as a separate count;

          a detecting part for outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

          a filter apparatus main body for outputting each of the plaintext when a detection signal is not outputted from the detecting part, and for holding the further output of ~~the plaintext~~ each of the plurality of plaintexts until it receives a process restart signal for instructing a restart of outputting each of the plurality of plaintext when the detection signal that shows the encryption algorithm is susceptible to a decryption attack is outputted.

15

5. (Currently Amended) An encryption apparatus for executing an encryption algorithm that receives ~~plaintext~~ each of a plurality of plaintexts to output ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

a receiving part for receiving the plurality of the plaintext plaintexts sequentially;

5 a counter part for separating a predetermined part from a bit string forming the ~~plaintext~~ each of the plurality of plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted ~~plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts~~ plurality of plaintexts each of which has a same value as the fixed  
10 part, and storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a predetermined number;

an encryption apparatus main body for performing the encryption algorithm for  
15 encryption of those plurality of plaintexts subject to the detecting part and when a the detection  
signal is not outputted from the detecting part, and for holding output of the plaintext any  
plurality of plaintexts when the detection signal is outputted;

an indication signal receiving part for receiving an indication signal for indicating  
[[an]] a change in the encryption algorithm for new-use subsequent encryption; and

20 a setting part for outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information required for setting information corresponding to the encryption algorithm for the

fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal,

25                    wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting information.

6.        (Currently Amended) An encryption apparatus for executing an encryption algorithm that receives ~~plaintext~~ a plurality of plaintexts to calculate ciphertext with a key, the encryption apparatus comprising:

                 a receiving part for receiving a plurality of the ~~plaintext~~ plaintexts sequentially;

5                    a counter part for separating a predetermined part from a bit string forming ~~the plaintext~~ each of the plurality of plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted ~~plaintext having a value of the fixed part included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts~~ plaintexts each of which has the same value of the fixed part, and  
10                    storing it as a separate count;

                 a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a predetermined number; and

                 an encryption apparatus main body for updating the key used for encryption when  
15                    a detection signal is outputted from the detecting part.

7.        (Currently Amended) A ciphertext storing apparatus for executing an encryption algorithm that receives ~~plaintext~~ a plurality of plaintexts to calculate ciphertext with a key, and storing the ciphertext, the ciphertext storing apparatus comprising:

a receiving part for receiving the plurality of the plaintext plaintexts sequentially;  
5 a counter part for separating a predetermined part from a bit string forming the  
plaintext each of the plurality of plaintexts into a fixed part and a remaining part into a variable  
part, counting the number of inputted plaintext having a value of the fixed part included in a set  
of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality  
of the values of the fixed parts plaintexts each of which has the same value of the fixed part, and  
10 storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption  
algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a  
predetermined number;

a ciphertext storing part allowed to store ciphertext; and  
15 a ciphertext storing apparatus main body for updating the key used for encryption  
when a detection signal is outputted from the detecting part, and for storing partial-plaintext  
partially each of the plurality of plaintexts, being a part of the plaintext the ciphertext, and key  
reference information allowing reference of the key having been used for encryption in the  
ciphertext storing part.

8. (Currently Amended) A filter apparatus for limiting output of ciphertext from a  
block encryption algorithm that receives and stirs plaintext each of a plurality of plaintexts with a  
key step by step to perform encryption and outputs ciphertext, the filter apparatus comprising:

a receiving part for receiving the plurality of the plaintext plaintexts sequentially;  
5 a counter part for separating a predetermined part from a bit string forming the  
plaintext each of the plurality of plaintexts into a fixed part and a remaining part into a variable

part, counting the number of inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of the fixed parts plaintexts each of which has the same value of the fixed part, and

10 storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a predetermined number; and

a filter apparatus main body for outputting the plaintext each of the plurality of  
15 plaintexts when a detection signal is not outputted from the detecting part, and for holding an  
output of the plaintext each of the plurality of plaintexts until it receives a process restart signal  
for instructing a restart of outputting the plaintext each of the held plurality of plaintexts when  
the detection signal is outputted.

9. (Currently Amended) An encryption apparatus for executing a block encryption algorithm that receives and stirs plaintext each of a plurality of plaintexts with a key, step by step, to perform encryption and outputs ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

5 a receiving part for receiving the plurality of the plaintext plaintexts sequentially;

a counter part for separating a predetermined part from a bit string forming the plaintext each of the plurality of plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintext having a value of the fixed part included in a set of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality

10 of the values of the ~~fixed parts~~ plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a predetermined number;

15 an encryption apparatus main body for executing the encryption algorithm for encryption when a detection signal is not outputted from the detecting part, and for holding output of the ~~plaintext~~ each of the plurality of plaintexts when the detection signal is outputted;

an indication signal receiving part for receiving an indication signal for indicating [[an]] a change in the encryption algorithm for new-use subsequent encryption; and

20 a setting part for outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information for setting information corresponding to the encryption algorithm for the fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal,

25 wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting information.

10. (Currently Amended) An encryption apparatus for executing a block encryption algorithm that receives and stirs ~~plaintext~~ each of plaintexts with a key, step by step, to perform encryption and outputs ciphertext, the encryption apparatus comprising:

a receiving part for receiving a plurality of the ~~plaintext~~ plaintexts sequentially;



5 a counter part for separating a predetermined part from a bit string forming the  
plaintext each of plaintexts into a fixed part and a remaining part into a variable part, counting  
the number of inputted plaintext having a value of the fixed part included in a set of values of the  
fixed parts at every set of the values of the fixed parts formed of 1 or a plurality of the values of  
the fixed parts plaintexts each of which has the same value of the fixed part, and storing it as a

10 separate count;

a detecting part for outputting a detection signal that shows the encryption  
algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a  
predetermined number; and

an encryption apparatus main body for updating the key used for encryption when  
15 a detection signal is outputted from the detecting part.

11. (Currently Amended) A ciphertext storing apparatus for executing a block  
encryption algorithm that receives and stirs plaintext each of a plurality of plaintexts with a key,  
step by step, to perform encryption and outputs ciphertext, and storing the ciphertext, the  
ciphertext storing apparatus comprising:

5 a receiving part for receiving the plurality of the plaintext plaintexts sequentially;

a counter part for separating a predetermined part from a bit string forming the  
plaintext each of the plurality of plaintexts into a fixed part and a remaining part into a variable  
part, counting the number of inputted plaintext having a value of the fixed part included in a set  
of values of the fixed parts at every set of the values of the fixed parts formed of 1 or a plurality  
10 of the values of the fixed parts plaintexts each of which has the same value of the fixed part, and  
storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a predetermined number;

15 a ciphertext storing part ~~allowed to store~~ storing ciphertext; and

a ciphertext storing apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing ~~partial-plaintext partially each of the plurality of plaintexts, being a part of the plaintext~~ the ciphertext, and key reference information allowing reference of the key having been used for encryption in the  
20 ciphertext storing part.

12. (Currently Amended) A filter apparatus for limiting an output of ciphertext from a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives a plurality of plaintext plaintexts sequentially, has a plurality of stirring steps for stir with a key, and performs  
5 encryption step by step to output ciphertext, the filter apparatus comprising:

a receiving part for receiving the plurality of the plaintext plaintexts sequentially;

a counter part for separating 17th to 32nd bits of each of the plaintext ~~from the plaintext plurality of plaintexts~~ into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the number of inputted ~~plaintext having a value of the fixed part~~  
10 ~~included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts~~ plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a

15 predetermined number; and

a filter apparatus main body for outputting each of the plaintext when a detection signal is not outputted from the detecting part, and for holding the further output of ~~the plaintext~~ each of the plurality of plaintexts until it receives a process restart signal for instructing a restart of outputting ~~the plaintext~~ each of the plurality of plaintexts when the detection signal is

20 outputted.

13. (Currently Amended) An encryption apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives a plurality of plaintext plaintexts sequentially, has a plurality of stirring steps for stir with a key, and performs encryption step by

5 step to output ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

a receiving part for receiving plurality of the plaintext plaintexts sequentially;

a counter part for separating 17th to 32nd bits of the ~~plaintext~~ each of the plurality of the plaintexts ~~from the plaintext~~ into a fixed part and first to 16th bits and 33rd to 64th bits

10 thereof into a variable part, counting the number of inputted ~~plaintext~~ having a value of the fixed part included in a set of values of the fixed parts formed of 1 or a plurality of the values of the fixed parts at every set of the values of the fixed parts plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption  
15 algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a  
predetermined number;

an encryption apparatus main body for executing the encryption algorithm for  
encryption ~~when a of those plurality of plaintexts subject to the detecting part and the~~ detection  
signal is not outputted from the detecting part, and for holding an output of the plaintext each of  
20 the plurality of plaintexts when the detection signal is outputted;

an indication signal receiving part for receiving an indication signal for indicating  
[[an]] a change in the encryption algorithm for new-use subsequent encryption; and

a setting part for outputting cipher setting information required for setting the  
encryption algorithm executed by the encryption apparatus main body and counter part setting  
25 information required for setting information corresponding to the encryption algorithm for the  
fixed part ~~and the set of the values of the fixed parts~~ and used by the counter part based on the  
indication signal,

wherein the encryption apparatus main body and the counter part perform the  
settings based on the cipher setting information and the counter part setting information.

14. (Currently Amended) An encryption apparatus for executing a KASUMI type  
encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to  
KASUMI which is a block encryption algorithm that receives plaintext each of a plurality of  
plaintexts, has a plurality of stirring steps for stir with a key, and performs encryption step by  
5 step to output ciphertext, the encryption apparatus comprising:

a receiving part for receiving the plurality of the plaintext plaintexts sequentially;

a counter part for separating 17th to 32nd bits of ~~the plaintext~~ each of the plurality of plaintexts from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the number of inputted ~~plaintext having a value of the fixed part~~ plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a predetermined number; and

an encryption apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part.

15. (Currently Amended) A ciphertext storing apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives ~~plaintext~~ each of a plurality of plaintexts, has a plurality of stirring steps for stir with a key, and performs encryption, step by step, to output ciphertext, and storing the ciphertext, the ciphertext storing apparatus comprising:

a receiving part for receiving the plurality of the plaintext plaintexts sequentially;

a counter part for separating 17th to 32nd bits of ~~the plaintext~~ each of the plurality of the plaintexts from the plaintext into a fixed part and first to 16th bits and 33rd to 64th bits thereof into a variable part, counting the number of inputted ~~plaintext having a value of the fixed part~~ plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

~~fixed parts at every set of the values of the fixed parts~~ plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part for outputting a detection signal that shows the encryption algorithm is susceptible to a decryption attack when at least one of the separate counts exceeds a  
15 predetermined number;

a ciphertext storing part allowed to store ciphertext; and

a ciphertext storing apparatus main body for updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing ~~partial plaintext being a part of the plaintext~~ partially each of the plurality of plaintexts, the ciphertext, and key  
20 reference information allowing reference of the key having been used for encryption in the ciphertext storing part.

16. (New) A plaintext detector system for analyzing potential susceptibility for blocks of plaintext, to be encrypted by an encryption algorithm, of being decrypted by an unauthorized party and increasing the security of the encryption of such plaintext, comprising:

a receiving unit for receiving a block of plaintext to be encrypted;

5 a counter unit connected to the receiving unit to separate, from the block of plaintext, a predetermined bit string, and to compute a value based on counting the predetermined bit string as virtually continuing bits to represent a susceptibility standard of unauthorized decryption; and

a detecting unit for comparing the computed value with a predetermined stored  
10 value wherein the block of plaintext that is less than the susceptibility standard predetermined stored value is provided a first signal that will permit encryption and the block of plaintext that is

equal or greater than the susceptibility standard predetermined stored value is provided a second signal to change a manner of execution of the encryption algorithm of the block of plaintext to increase security.

17. (New) The plaintext detector system of Claim 16 where the second signal enable a change of a key used by the encryption algorithm.